



10/082758  
09-12-07

COFC

Docket No.: 09469/014001; 97.0013  
(PATENT)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Letters Patent of:  
Chui-Shan Teresa Lam et al.

Patent No.: 7,251,635

Issued: July 31, 2007

For: METHOD AND APPARATUS FOR  
MANAGING A KEY MANAGEMENT  
SYSTEM

**Certificate**  
SEP 14 2007  
**of Correction**

**REQUEST FOR CERTIFICATE OF CORRECTION  
PURSUANT TO 37 CFR 1.322**

Attention: Certificate of Correction Branch  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

Upon reviewing the above-identified patent, Patentee noted typographical errors which should be corrected.

In the Claims:

In Claim 1, column 10, line 10, before the word "value", the word "key" is erroneously missing.

In claim 1, column 10, line 12, before the word "value", the word "key" is erroneously missing.

In claim 1, column 10, line 20, before the word "value", the word "key" is erroneously missing.

SEP 14 2007

In claim 1, column 10, line 36, before the word “value”, the word “key” is erroneously missing.

In claim 1, column 10, line 38, before the word “value”, the word “key” is erroneously missing.

In claim 4, column 10, line 64, before the word “value”, the word “key” is erroneously missing.

In claim 4, column 10, line 66, before the word “value”, the word “key” is erroneously missing.

In claim 4, column 11, line 7, before the word “value”, the word “key” is erroneously missing.

In claim 4, column 11, line 24, before the word “value”, the word “key” is erroneously missing.

In claim 4, column 11, line 26, before the word “value”, the word “key” is erroneously missing.

The errors were not caused by the applicants; accordingly no fee is required.

Transmitted herewith is a proposed Certificate of Correction effecting such amendment. Also enclosed, as evidence of the error, is a copy of the claims in the issued patent and page 2 of the Notice of Allowance, which shows the Examiner’s Amendment. Patentee respectfully solicits the granting of the requested Certificate of Correction.

SEP 14 2007


Patent No.: 7,251,635

Docket No.: 09469/014001; 97.0013

Applicants believe no fee is due with this request. However, if a fee is due, please charge our Deposit Account No. 50-0591, under Order No. 09469/014001.

Dated: September 11, 2007

Respectfully submitted,

By  <sup>\$ L0031</sup> ALY DOSSA  
Robert P. Lord

Registration No.: 46,479  
OSHA · LIANG LLP  
1221 McKinney St., Suite 2800  
Houston, Texas 77010  
(713) 228-8600  
(713) 228-8778 (Fax)

SEP 14 2007

proceeds to retrieve and de-serialize a serialized file from the KMS storage specifically using the serialization module (Step 120). The KEK is subsequently hashed by the hashing module (Step 124). The hash of the KEK obtained from the input source is compared to the KEK Hash (Step 126). If the hash of the KEK obtained from the input source is not equal to the KEK Hash, then access to the KMS is denied (Step 128).

If the hash of the KEK obtained from the input source is equal to the KEK Hash, then access to the KMS is granted and the KMS proceeds to decrypt the secret tokens to produce tuples (Step 130). The encryption module is used to decrypt the secret tokens. The tuples are then stored in a hash table data structure created within the memory (Step 132). Those skilled in the art will appreciate that any data structure may be used to store the tuples in the memory. If the KMS is running (Step 116) or once steps 118 through 132 have been completed, the tuple corresponding to the requested key is retrieved (Step 134). The tuple is subsequently forwarded to the requesting application (Step 136).

FIG. 12 illustrates the typical steps involved in changing a KEK within a Key Management System in accordance with one embodiment of the invention. A user enters old and new KEK information into a Change KEK for Key Management Service GUI (Step 180). A serialized file associated with the old KEK is de-serialized (Step 182). An old KEK is hashed (Step 184). The old KEK is associated with the old KEK information entered by the user in Step 180. A comparison is made of a hash of the old KEK (as entered in Step 180) and a hashed KEK included in a vector stored in a KMS Storage associated with the KMS (Step 186). A determination is made as to whether the hash of the old KEK entered by the user is the same as the hash of the KEK associated with the vector (Step 188). If the hash of the old KEK entered by the user is not the same as the hash of the KEK associated with the vector, then the procedure may be terminated (Step 190). Alternatively, the user may be prompted to re-enter old and new KEK information. Otherwise, if the hash of the old KEK entered by the user is the same as the hash of the KEK associated with the vector, one or more secret tokens included in the vector are decrypted using the old KEK (Step 192). One or more secret tokens included in the vector are subsequently encrypted using the new KEK (Step 194). The new KEK is hashed (Step 196). A serialized file including the new KEK hash, the secret tokens and the encoded key list is subsequently created (Step 196). The KMS may then be restarted using the new KEK (Step 200). One skilled in the art will recognize that the order and functionality of the steps presented in FIG. 12 may vary in accordance with a particular embodiment of the present invention.

Advantages of the invention may include one or more of the following. In some embodiments, the invention provides a software solution to key management systems. Further, the invention may be integrated into existing network infrastructure without requiring additional hardware. In some embodiments, the invention is scalable to manage keys for multiple applications. In some embodiments, the invention allows sensitive data to be readily backed-up and recovered. In some embodiments of the invention, the keys are never stored as clear text. Further, the invention allows the KMS to be distributed over multiple servers within a network system. Further, the invention allows the KEK to contain multiple portions, e.g., salt, count, integer, such that KEK may be distributed to multiple security officers. In some embodiments, the invention allows the key management system to be modified without replacing or modifying any hardware components. Those skilled in the art can appreciate that the invention may include other advantages and features.

While the invention has been described with respect to a limited number of embodiments, those skilled in the art, having benefit of this disclosure, will appreciate that other embodiments can be devised which do not depart from the scope of the invention as disclosed herein. Accordingly, the scope of the invention should be limited only by the attached claims.

What is claimed is:

1. A method for retrieving a value secured in a key management system comprising:
  - receiving a request for the value secured in the key management system;
  - retrieving a serialized file from a key management system storage;
  - de-serializing the serialized file producing a de-serialized file;
  - decoding an encoded key list in the de-serialized file to produce a decoded key list;
  - searching for a key corresponding to the value in the decoded key list;
  - inputting a key encryption key into the key management system;
  - hashing the key encryption key to produce a key encryption key hash, wherein the key encryption key hash is equal to a hashed key encryption key in the de-serialized file;
  - comparing the key encryption key hash to the hashed key encryption key in the de-serialized file to grant access to the key management system;
  - decrypting a secret token in the de-serialized file using the key encryption key to produce at least one tuple after access to the key management system is granted;
  - storing the at least one tuple in a data structure within the key management system; and
  - retrieving a tuple corresponding to the value from the at least one tuple, using the key corresponding to the value.
2. The method of claim 1, further comprising:
  - searching a local file system, for the key when the key is not found in the decoded key list.
3. A method for changing an existing key encryption key, comprising:
  - entering the existing key encryption key;
  - entering a new key encryption key;
  - de-serializing a serialized file producing a de-serialized file;
  - hashing the existing key encryption key producing a hashed key encryption key, wherein the hashed key encryption key is equal to a key encryption key hash in the de-serialized file;
  - comparing the hashed key encryption key to the key encryption key hash in the de-serialized file to grant access to a key management system;
  - decrypting a secret token using the existing key encryption key to produce a tuple after access to the key management system is granted;
  - encrypting the tuple using the new key encryption key producing a new secret token;
  - hashing the new key encryption key producing a new hashed key encryption key; and
  - serializing the new hashed key encryption key and the new secret token to produce a new serialized file.
4. An apparatus for retrieving a value secured in a key management system comprising:
  - means for receiving a request for the value secured in the key management system;

SEP 14 2007

11

means for retrieving a serialized file from a key management system storage;  
 means for de-serializing the serialized file producing a de-serialized file;  
 means for decoding an encoded key list in the de-serialized file to produce a decoded key list;  
 means for searching for a key corresponding to the value in the decoded key list;  
 means for inputting a key encryption key into the key management system;  
 means for hashing the key encryption key to produce a key encryption key hash, wherein the key encryption key hash is equal to a hashed key encryption key in the de-serialized file;  
 means for comparing the key encryption key hash to the hashed key encryption key in the de-serialized file to grant access to the key management system;  
 means for decrypting a secret token in the de-serialized file using the key encryption key to produce at least one tuple after access to the key management system is granted;  
 means for storing the at least one tuple in a data structure within the key management system; and  
 means for retrieving a tuple corresponding to the value from the at least one tuple, using the key corresponding to the value.

12

5. An apparatus for changing an existing key encryption key, comprising:  
 means for entering the existing key encryption key;  
 means for entering a new key encryption key;  
 means for de-serializing a serialized file producing a de-serialized file;  
 means for hashing the existing key encryption key producing a hashed key encryption key,  
 wherein the hashed key encryption key is equal to a key encryption key hash in the de-serialized file;  
 means for comparing the hashed key encryption key to the key encryption key hash in the de-serialized file to grant access to a key management system;  
 means for decrypting a secret token using the existing key encryption key to produce a tuple after access to the key management system is granted;  
 means for encrypting the tuple using the new key encryption key producing a new secret token;  
 means for hashing the new key encryption key producing a new hashed key encryption key; and  
 means for serializing the new hashed key encryption key and the new secret token to produce a new serialized file.

\* \* \* \* \*

Art Unit: 3621

**DETAILED ACTION**

An Examiner's Amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this Examiner's amendment was given in a telephone interview with Robert Lord on March 19, 2007.

The claims are amended as follows:

Claim 30,

A method for retrieving a key value secured in a key management system comprising: receiving a request for the key value secured in the key management system; retrieving a serialized file from a key management system storage; de-serializing the serialized file producing a de-serialized file; decoding an encoded key list in the de-serialized file to produce a decoded key list; searching for a key corresponding to the key value in the decoded key list; inputting a key encryption key into the key management system; hashing the key encryption key to produce a key encryption key hash, wherein the key encryption key hash is equal to a hashed key encryption key in the de-serialized file; comparing the key encryption key hash to the hashed key encryption key in the de-serialized file to grant access to the key management system; decrypting a secret token in the de-serialized file using the key encryption key to produce at least one tuple after access to the key management system is granted; storing the at least one tuple in a data structure within the key management system; and retrieving a tuple corresponding to the key value from the at least one tuple, using the key corresponding to the key value.

Claim 34,

An apparatus for retrieving a key value secured in a key management system comprising: means for receiving a request for the key value secured in the key management system; means for retrieving a serialized file from a key management system storage; means for de-serializing the serialized file producing a de-serialized file; means for decoding an encoded key list in the de-serialized file to produce a decoded key list; means for searching for a key corresponding to the key value in the decoded key list; means for inputting a key encryption key into the key management system; means for hashing the key encryption key to produce a key encryption key hash, wherein the key encryption key hash is equal to a hashed key encryption key in the de-serialized file; means for comparing the key encryption key hash to the hashed key encryption key in the de-serialized file to grant access to the key management system; means for decrypting a secret token in the de-serialized file using the key encryption key to produce at least one tuple after access to the key management system is granted; means for storing the at least one tuple in a data structure within the key management system; and means for retrieving a tuple corresponding to the key value from the at least one tuple, using the key corresponding to the key value.

SEP 14 2007

**UNITED STATES PATENT AND TRADEMARK OFFICE  
CERTIFICATE OF CORRECTION**

Page 1 of 1

PATENT NO. : 7,251,635  
APPLICATION NO. : 10/082,758  
ISSUE DATE : July 31, 2007  
INVENTOR(S) : Chui-Shan Teresa Lam et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the claims:

In claim 1, column 10, line 10, before the word "value", the word "key" is erroneously missing.

In claim 1, column 10, line 12, before the word "value", the word "key" is erroneously missing.

In claim 1, column 10, line 20, before the word "value", the word "key" is erroneously missing.

In claim 1, column 10, line 36, before the word "value", the word "key" is erroneously missing.

In claim 1, column 10, line 38, before the word "value", the word "key" is erroneously missing.

In claim 4, column 10, line 64, before the word "value", the word "key" is erroneously missing.

In claim 4, column 10, line 66, before the word "value", the word "key" is erroneously missing.

In claim 4, column 11, line 7, before the word "value", the word "key" is erroneously missing.

In claim 4, column 11, line 24, before the word "value", the word "key" is erroneously missing.

In claim 4, column 11, line 26, before the word "value", the word "key" is erroneously missing.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

Robert P. Lord  
OSHA · LIANG LLP  
1221 McKinney St., Suite 2800  
Houston, Texas 77010

1

SEP 14 2007



Application No. (if known): 10/082,758

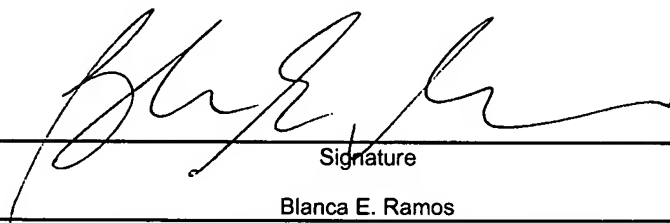
Attorney Docket No.: 09469/014001

## Certificate of Express Mailing Under 37 CFR 1.10

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Airbill No. EM011787671US in an envelope addressed to:

Attention: Certificate of Correction Branch  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

on September 11, 2007  
Date



Signature

Blanca E. Ramos

Typed or printed name of person signing Certificate

Registration Number, if applicable

(713) 228-8600  
Telephone Number

Note: Each paper must have its own certificate of mailing, or this certificate must identify each submitted paper.

Request for Certificate of Correction (No Fee) with attachments (6 pages)  
Certificate of Correction (1 page)  
Return Receipt Postcard

SEP 14 2007